UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/853,465
Filing Date: May 11, 2001
Appellant(s): STRONGIN, GEOFFREY S.

Mark W. Sincell, Ph. D.
Reg. No. 52,226
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11 April 2006 appealing from the Office action mailed November 15, 2005. This is a revised Examiner's Answer to fix the headings in accordance with Order returning Examiner's Answer of July 20, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is deficient. 37 CFR 41.37(c)(1)(v) requires the summary of claimed subject matter to include: (1) a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number, and to the drawing, if any, by reference characters and (2) for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function as permitted by 35 U.S.C. 112, sixth paragraph, must be identified and the structure, material, or acts described in the specification as corresponding to each claimed function must be set forth with reference to the specification by page and line number, and to the drawing, if any, by reference characters. The brief is deficient because: the summary of invention contained in the

brief, is not reflected in the claims presented. The claims presented are very broad and contain a 112 second paragraph rejection because it is unclear what applicant is claiming as his invention. The brief contains specific examples from the specification (pages 71-72 and 31) and drawing (Figures 7C, 7D, 27) presented in the disclosure but not reflected in the claims. Note the disclosure contains 73 sheets of drawings and 104 pages of specification.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Vu, et al. (U.S. Patent No. 6,557,104)

U.S. Patent Application Publication Mathis, Richard M. 2001/0037438

Kai, Nobuhiro (U.S. Patent No. 6,230,244)

Takata, Hidekazu (U.S. Patent No. 6,469,928)

Phillips et al. (U.S. Patent No. 6,505,279)

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

The 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement placed on Claims 1-103 in Final Rejection is withdrawn because applicant points to Vu et al. (the prior art references used in the Final Rejection) col. 1, lines 12-33 as teaching that "secret" information can be interpreted as "key" or other means of verification such as a signature.

Claims 1-38 and 51-103 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In the claims the following text from claim 1 is unclear

"the method comprising: reading a secret from a first location; securing the secret in a secure location different from the first location; and retrieving at least a portion of the data stored in the first location using the secret". It is unclear to the Examiner if the secret is removed from the first location when it is placed in a "secure location different that the first location" furthermore, it is unclear if the secret in the first location is used to retrieve the data stored in the first location or the secret secured in location different is used to retrieve the data stored in the first location. Furthermore the claims do not indicate what is done with the retrieved data.

The following text from claim 32 is unclear

"storing a secret within a first location; and storing code different from the secret within the first location; wherein the code is configured to provide access to data stored in the first location when processed in association with the secret" It is unclear if the first location here is equal to the "location different than the first location, i.e. the SRAM" in previously presented claim 1, and "storing code different" is equivalent to the "data retrieved" in claim 1.

Claims 1-103 are rejected under 35 U.S.C. 103(a). This is new grounds of rejection that utilize prior art references the primary reference is the same reference used in a 102(e) rejection of the Final Rejection, in addition the other reference was presented to Applicant on

15 December 2004. The motivation to combine these references is shown in the primary reference Vu et al. col. 6, lines 3-21 which indicate that a key and program can be loaded into secure memory either at boot time or at later times for implementation where a computer has multiple users. Vu also indicates in col. 6, lines 3-21 "Those skilled in the art will appreciate that numerous possible variations of loading and processing the cryptographic keys and programs are possible, which are within the scope of the present invention, as long as the loading and processing are performed in the secure processor mode using the secure memory". The key is interpreted to be the secret; the program is interpreted to be the data. The Mathis application is directed to computer memory protection related to consumer interactive devices such as gaming machines, the Mathis application shows that a secret is used to retrieve data from a second location.

Regarding claims 1-103, the stated rejection is based upon Vu, et al. U.S. Patent No. 6,557,104 (hereinafter Vu) in view of U.S. Patent Application Publication Mathis, Richard M. 2001/0037438 (hereinafter Mathis).

As per the first limitation of claim 1, **"A method of securely accessing data in a personal computer, the method comprising:"** is taught in Vu col. 3, lines 53-67;

As per the second limitation of claim 1, **"reading a secret from a first location; securing the secret in a secure location different from the first location"** is shown in Vu col. 4, lines 21-67 (note in this claim the first location is considered to be equivalent to the "token", and the "storing code different from the secret" is interpreted to be equivalent to the "SMRAM").

As per the third limitation of claim 1, "**and; retrieving at least a portion of the data stored in the first location using the secret"** is taught in Mathis on pages 2-3, paragraphs 0014-

0020 "A secure memory device (SMD) is provided that comprises means to independently read the program memory device and compute and store a signature or other means of verification of binary content of the program memory device, means to compare binary program memory content to binary program memory content stored in the program memory device, and means to disable reading and writing of the program memory device if predetermined conditions do not occur … Advantages of the present invention include the following: provide independent means of verification of microcomputer program memory content by other than manual means; restrict microcomputer access to program memory content that has been determined to be incorrect and to prevent operation of an apparatus containing the incorrect program memory" (Note: 'disable reading and writing when predetermined conditions do not occur' is interpreted to have the same meaning as 'providing access in association with the secret').

Claims 2-31, 52-54, 56-63, and 67-77 all stand or fall with claim 1.

Claims 51, 55, and 66, are independent claims containing limitation similar to those present in claim 1.

Regarding claim 32, the stated rejection is based upon Vu, et al. U.S. Patent No. 6,557,104 (hereinafter Vu) in view of U.S. Patent Application Publication Mathis, Richard M. 2001/0037438 (hereinafter Mathis).

As per the first limitation of claim 32, **"A method of securing data in a personal computer system, the method comprising:"** is taught in Vu col. 3, lines 53-67;

As per the second limitation of claim 32, **"storing a secret within a first location; and storing code different from the secret within the first location"** is shown in Vu col. 4, lines 21-36 (note in this claim the first location is considered to be equivalent to the "token", and

the "storing code different from the secret" is interpreted to be equivalent to the "other information" contained on the token)

As per the third limitation of claim 32, **"wherein the code is configured to provide access to data stored in the first location when processed in association with the secret"** is taught in Mathis on pages 2-3, paragraphs 0014-0020 "A secure memory device (SMD) is provided that comprises means to independently read the program memory device and compute and store a signature or other means of verification of binary content of the program memory device, means to compare binary program memory content to binary program memory content stored in the program memory device, and means to disable reading and writing of the program memory device if predetermined conditions do not occur … Advantages of the present invention include the following: provide independent means of verification of microcomputer program memory content by other than manual means; restrict microcomputer access to program memory content that has been determined to be incorrect and to prevent operation of an apparatus containing the incorrect program memory" (Note: 'disable reading and writing when predetermined conditions do not occur' is interpreted to have the same meaning as 'providing access in association with the secret').

Claims 33-38, 65, and 98-103 all stand or fall with claim 1. Claims 64 and 97 are independent claims containing limitation similar to those present in claim 32.

As per the first limitation of claim 39, **"A personal computer system comprising:"** is taught in Vu col. 3, lines 53-67;

As per the second limitation of claim 39, **"a first location configured to store code, a secret, and data different from the secret and different from the code"** is shown in Vu col. 4,

lines 21-36 (note in this claim the first location is considered to be equivalent to the "token", and the "storing data different from the secret and the code" is interpreted to be equivalent to the "other information" contained on the token)

As per the third limitation of claim 39 **"a master device operable coupled to the first location, wherein the master device is configured to read the secret from the first location and to store the secret in a secure location different from the fist location"** is shown in Vu col. 4, lines 21-67 (note in this claim the first location is considered to be equivalent to the "token", and the "storing code different from the secret" is interpreted to be equivalent to the "SMRAM").

As per the fourth limitation of claim 39, **"and where the master device is futher configured to access the data stored in the first location using the secret"** is taught in Mathis on pages 2-3, paragraphs 0014-0020 "A secure memory device (SMD) is provided that comprises means to independently read the program memory device and compute and store a signature or other means of verification of binary content of the program memory device, means to compare binary program memory content to binary program memory content stored in the program memory device, and means to disable reading and writing of the program memory device if predetermined conditions do not occur … Advantages of the present invention include the following: provide independent means of verification of microcomputer program memory content by other than manual means; restrict microcomputer access to program memory content that has been determined to be incorrect and to prevent operation of an apparatus containing the incorrect program memory" (Note: 'disable reading and writing when predetermined conditions

do not occur' is interpreted to have the same meaning as 'providing access in association with the secret').

Claims 40-49 all stand or fall with claim 39.

(10) Response to Argument

Regarding Appellant's first argument beginning on page 6, "the Examiner alleges that the use of a secret is not enabled. Applicant respectfully disagrees and submits that the use of secret information to protect confidential information is well-known. Furthermore, the secret information may take a variety forms. Support for this position may be found in the references cited by the Examiner. See e.g., Vu, col. 1, ll 11-33". The Examiner has removed the 112 first enablement rejection.

Regarding Appellant's second argument beginning on page 7, "The Examiner also alleges that specification does not describe what function or uses are performed when retrieving the data from the first location. Applicant respectfully submits that some embodiments of the present invention set forth techniques for accessing data stored in a first location using a secret … Applicant therefore submits that the claims are definite and requests that the Examiner's rejections of claim 1-103 under 35 § U.S.C. 112, second paragraph, be REVERSED." The Examiner disagrees with argument and notes the claims as written are indefinite, the details from the specification relied upon for explanation need to be incorporated in the claims in order to convey the invention. The rejection above in paragraph (9) provides more details to the 112, second paragraph rejection placed on the claims.

Regarding Appellant's third argument beginning on page 8 with regard to independent claim 1, "Applicant respectfully submits that Vu fail to teach or suggest reading a secret from a

first location, securing the secret in a secure location different from the first location, and retrieving at least a portion of the data stored in the first location using the secret". As noted above the claims as presented contain a 112 second paragraph rejection, as best interpreted by the Examiner the following rejection shows these functions:

"reading a secret from a first location; securing the secret in a secure location different from the first location" is shown in Vu col. 4, lines 21-67(note in this claim the first location is considered to be equivalent to the "token", and the "storing code different from the secret" is interpreted to be equivalent to the "SMRAM").

"**and; retrieving at least a portion of the data stored in the first location using the secret"** is taught in Mathis on pages 2-3, paragraphs 0014-0020 (Note: 'disable reading and writing when predetermined conditions do not occur' is interpreted to have the same meaning as 'providing access in association with the secret').

The motivation to combine these references is shown in the primary reference Vu et al. col. 6, lines 3-21 which indicate that a key and program can be loaded into secure memory either at boot time or at later times for implementation where a computer has multiple users. The key is interpreted to be the secret; the program is interpreted to be the data. The Mathis application is directed to computer memory protection related to consumer interactive devices such as gaming machines, the Mathis application shows that a secret is used to retrieve data from a second location.

Regarding Appellant's fourth argument on page 9 with regard to independent claim 1, "In the Final Office Action, the Examiner confirms the above analysis of Vu … Third, the Examiner states that the data is accessed from the SMRAM, i.e., the "the secure location different than the

first location," using the cryptographic key. See Final Office Action page 5. Thus Vu does not teach that the cryptographic key is used to access the cryptographic program or any other data or information that may be stored on the physical token. To the contrary, the cryptographic key is used to access information from the SMRAM and not from the physical token, i.e., the "first location" identified by the Examiner. In fact it, is impossible to access information stored on the physical token because the physical token is removed to ensure system integrity once the cryptographic key as been stored in the SMRAM". The Examiner disagrees with argument for multiple reasons. One the Applicant misinterpreted the Final Office Action on page 5, the Examiner was relaying that the information on the token i.e., data can be retrieved at other times see Vu col. 6, lines 6-21, on page 3 of the Final Office Action. Two the rejection has been expanded to include another reference to show that the secret can be used to determine whether to access the data. Third the claim as written is indefinite is the secret used on the token used to access the data or is the secret that is secured in the different location used to access the data on the token? Fourth, Vu indicates that the token can be removed or attached while operating in secure mode see col. 6, lines 6-21 as well as col. 6, lines 63-67 where the user is requested to insert a token.

Regarding Appellant's fifth argument on page 9 with regard to claim 32, "Applicant also submits that Vu fails to teach or suggest storing a secret within a first location and storing code different from the secret within the first location, where the code is configured to provide access to data stored in the first location when processed in association with the secret". As indicated in the above rejection the 112 second paragraph rejections apply as well as the new grounds of rejection which utilize a 103 with Vu as the primary reference in combination with Mathis.

Regarding Appellant's sixth argument on page 10 with regard to claim 39, "that Vu fails to teach or suggest a first location configured to store code, a secret, and data different from the secret and different from the code, and a master device operable coupled to the first location, wherein the master device is configured to read the secret from the first location and to store the secret in a secure location different from the first location, and where the master device is further configured to access the data stored in the first location using the secret, as set forth in independent claim 39". The Examiner disagrees with applicant the rejection in paragraph 9, with the combination of Vu and Mathis teaches these limitations.

For the above reasons, it is believed that the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

/ELLEN TRAN/
Primary Examiner, Art Unit 2433

Conferees:

Kambiz Zand

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436